ABSTRACT

A method for providing security with a secure chip, includes: creating a migratable keyblob using a first random number, where the migratable keyblob contains a key; wrapping the migratable keyblob with a public key of the key's parent key; encrypting the first random number with a pass phrase for a user of the key; storing the encrypted first random number; and migrating the migratable keyblob from the computer to itself. If the private key of the secure chip is stolen, the thief can only unwrap keys which are ancestors of the key in the migratable keyblob. To obtain the key in the migratable keyblob, the random number used to create it is required. However, the pass phrase of the user is required to decrypt it. This increases the security of the key stored in the migratable keyblob and its children keys.